

1                   **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2   Application Serial No. .... 10/670,298  
3   Filing Date ..... 09/26/2003  
4   Inventorship .....Klaes  
5   Group Art Unit.....2135  
6   Examiner .....SHAN, April Ying  
7   Attorney's Docket No. ....ER1-0014US  
8   Title: SECURITY MONITORING AND INTRUSION DETECTION SYSTEM

9                                   **APPEAL BRIEF**

10   To:   MS: Appeal Brief - Patents  
11        Commissioner for Patents  
12        P.O. Box 1450  
13        Alexandria, VA 22313-1450  
  
14   From: Tim R. Wyckoff  
15        **Customer No. 29150**  
16        Lee & Hayes PLLC  
17        421 W Riverside Avenue, Suite 500  
18        Spokane, WA 99201

19                                   **INTRODUCTORY COMMENTS**

20               Pursuant to 37 C.F.R. § 41.37, Appellant hereby submits an Appeal Brief  
21   for Application Serial No. 10/670,298 filed September 26, 2003. A Notice of  
22   Appeal was filed on December 10, 2007. Accordingly, Appellant appeals to the  
23   Board of Patent Appeals and Interferences (hereinafter "Board") seeking review of  
24   the Office's rejections.  
25

## TABLE OF CONTENTS

<u>Appeal Brief Items</u>	<u>Page</u>
(i) Real Party in Interest	4
(ii) Related Appeals and Interferences	4
(iii) Status of Claims	4
(iv) Status of Amendments	5
(v) Summary of Claimed Subject Matter	5
(vi) Grounds of Rejection to be Reviewed on Appeal	7
(vii) Argument	8
(A) Claims 1-30 fully conform with the 35 U.S.C. § 112, first paragraph written description requirement	8
(B) Claims 12-21 fully conform with the 35 U.S.C. § 112, first paragraph enablement requirement	11
(C) Claims 1-12 recite statutory subject matter, as required under 35 U.S.C. § 101	13
(D) Claims 1-7, 9-17, 19-28 and 30 are allowable because Khanolkar does not suggest the subject matter of these claims	14

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

(E) Claims 8, 18 and 29 are allowable 15  
because Khanolkar in view APA does  
not suggest the subject matter of these  
claims

(viii)	Claims Appendix	17
(ix)	Evidence Appendix	None
(x)	Related Proceedings Appendix	None

1                   **(i) Real Party in Interest**

2                   The real party in interest is the Swiss Reinsurance Corporation, the assignee  
3 of all right and title to the subject invention.

4  
5                   **(ii) Related Appeals and Interferences**

6                   Appellant is not aware of any other appeals or interferences which will  
7 directly affect, be directly affected by, or otherwise have a bearing on the Board's  
8 decision to this pending Appeal.

9  
10                  **(iii) Status of Claims**

11                  Allowed Claims: No claims have been allowed.

12                  Canceled Claims: No claims have been canceled.

13                  Originally Presented Claims: Claims 1-30 were originally presented when  
14 this Application was filed.

15                  Pending Claims: Claims 1-30 stand rejected and are pending in this  
16 Application as set forth in the Claims Appendix on page 17.

17                  Appealed Claims: All of the pending claims are subject to this Appeal.  
18 Claims 1-30 are rejected under 35 U.S.C. § 112, first paragraph, as failing to  
19 comply with the written description requirement. Claims 12-21 are rejected under  
20 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement  
21 requirement. Claims 1-21 are rejected under 35 U.S.C. § 101 because it is asserted  
22 that the claims are directed to non-statutory subject matter. Claims 1-7, 9-17, 19-  
23 28 and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over  
24 Khanolkar et al., U.S. Patent No. 7,127,743 (hereinafter "Khanolkar"). Claims 8,  
25 18 and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over

Khanolkar in view of "Admitted prior art" (hereinafter "APA"). The indicated rejections are set forth in the Final Office Action dated August 8, 2007.

**(iv) Status of Amendments**

An Amendment has not been filed subsequent to the Final Office Action dated August 8, 2007.

**(v) Summary of Claimed Subject Matter**

The following is a concise explanation of each independent claim 1, 12 and 22 and dependent claim 9 involved in the Appeal and includes, where appropriate, references to the specification (as filed) by page, paragraph and line number, and to the drawings. The claims are not to be limited solely to the elements identified by the reference characters and other related description.

**Claim 1** recites a computer-implemented monitoring/intrusion detection system, comprising: a central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*), at least one proxy loghost (*page 5, paragraph [0015], line 11; Figs. 1-3; proxy loghost 160*) remote (*page 7, paragraph [0024], line 5; Fig. 1; proxy loghost 160 shown remote*) from the central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*) and in communication with the central loghost over a network (*page 5, paragraph [0015], line 10; Fig. 1; network 150*); and at least one monitoring station (*page 9, paragraph [0028], line 1; Fig. 3; alarming module 310*), wherein the proxy loghost receives a plurality of log files (*See e.g., pages 4 & 5, paragraphs [0015] & [0015]*) from a plurality of resources (*page 4, paragraph [0015], line 1; Fig. 1; resources 170*) operating on the network, analyzes the log files for at least one of unexpected volume,

unexpected patterns, or unexpected types of log files (*See e.g., page 7, paragraph [0022]*), and generates events (*See e.g., pages 7 & 8, paragraphs [0025] & [0026]*) in view of such analysis, wherein the central loghost is operable to receive the events generated by the proxy loghost through the network and generate an alert (*See e.g., page 8, paragraph [0027]*) upon an analysis of the events, and wherein the monitoring station is caused to issue an alarm when the alert (*page 9, paragraph [0029], lines 11-12; Figs. 3 & 4; "alarm is 'sounded'"*) is generated.

**Claim 9** which depends from claim 1 recites that the log files are archived on the proxy loghost (*See e.g., pages 5 & 6, paragraphs [0018]*) and the events are archived (*page 6, paragraph [0019], line 5; Fig. 1; disk 200*) on the central loghost.

**Claim 12** recites a computer-implemented system for detecting intrusion into a secure network, comprising: a plurality of proxy loghosts (*page 5, paragraph [0015], line 11; Figs. 1-3; proxy loghost 160*), each proxy loghost collecting log files (*See e.g., pages 4 & 5, paragraphs [0015] & [0015]*) that are generated by resources in a portion of the secure network, the plurality of loghosts generating events (*See e.g., pages 7 & 8, paragraphs [0025] & [0026]*) in response to the log files collected; and a central loghost (*page 5, paragraph [0015], line 13; Figs. 1-3; central loghost 100*) remote (*page 7, paragraph [0024], line 5; Fig. 1; proxy loghost 160 shown remote*) from the plurality of proxy loghosts and in communication with the plurality of proxy loghosts over a network (*page 5, paragraph [0015], line 10; Fig. 1; network 150*), the central loghost receiving the log files themselves and the events from the plurality of proxy loghosts, the central loghost analyzing the log files and the events to determine the necessity of generating an alert (*See e.g., page 8, paragraph*

[0027]] and an associated alarm (page 9, paragraph [0029], lines 11-12; Figs. 3 & 4; "alarm is 'sounded'") to notify a security manager (See e.g., page 6, paragraph [0018]) of a possible intrusion incident.

**Claim 22** recites a method of monitoring a network, comprising: receiving a plurality of log messages at a proxy loghost (page 9, paragraph [0029], lines 1-2; Fig. 4; Block 410); analyzing the log messages and determining whether, in the log files, there exists any anomalies or unusual patterns (page 9, paragraph [0029], lines 3-4; Fig. 4; Block 420); generating an event in response to the anomalies or unusual patterns and forwarding the event over a network from the proxy loghost to a remote central loghost (page 9, paragraph [0029], lines 4-8; Fig. 4; Block 430); monitoring the events at the central loghost and generating an alert in accordance with predetermined event analysis (page 9, paragraph [0029], lines 8-13; Fig. 4; Block 450); and generating an alarm communication in coordination with the alert, the alarm being indicative of an unwanted incident in the network (page 9, paragraph [0029], lines 8-13; Fig. 4; Block 460).

**(vi) Grounds of Rejection to be Reviewed on Appeal**

**Claim Rejections Under 35 U.S.C. § 112**

Claims 1-30 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement.

Claims 12-21 are rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement.

**Claim Rejection Under 35 U.S.C. § 101**

Claims 1-21 are rejected under 35 U.S.C. § 101 because it is asserted that the claims are directed to non-statutory subject matter.

1 Claim Rejection Under 35 U.S.C. § 103

2 Claims 1-7, 9-17, 19-28 and 30 stand rejected under 35 U.S.C. § 103(a) as  
3 being unpatentable over Khanolkar.

4 Claims 8, 18 and 29 stand rejected under 35 U.S.C. § 103(a) as being  
5 unpatentable over Khanolkar in view of "Admitted prior art" (hereinafter "APA").

6  
7 (vii) Argument

8  
9 (A) Claims 1-30 fully conform with the 35 U.S.C. § 112, first  
10 paragraph written description requirement

11  
12 Independent claims 1, 12 and 22

13 Each of the rejected independent **claims 1, 12 and 22** recites that the  
14 central and proxy loghosts are "remote" from each other. The Office states  
15 Appellant's disclosure discloses that "both proxy and central loghosts" are  
16 "independent modules that can run on the same system," and therefore, the central  
17 and proxy loghosts are not remote from each other. (*See page 2, point 5, Office*  
18 *Action of August 2008*.) The Appellant respectfully submits the Office's  
19 understanding of the term "remote" is incorrect and that there is indeed support for  
20 the use of "remote" in the claims.

21 As those of ordinary skill in the computer related arts appreciate, the word  
22 "remote" does not necessarily describe or denote great distance between a plurality  
23 of elements. To the contrary, the word remote may simply mean that two or more  
24 elements, entities, or elements are spatially separate, but a great amount of  
25 separation is not required. Therefore, the Office's argument that "two computers



1 under the same system" and in very "close proximity" are not "remote" is not  
2 correct. Moreover, Wikipedia (wikipedia.org) defines "remote" computer as "a  
3 computer to which a user does not have physical access, but which he or she can  
4 access/manipulate via some kind of network from a local computer (one which the  
5 user does have physical access to)." As is shown in Fig. 1 of the instant  
6 Application, the central loghost 100 and the proxy loghost 160 are separated by  
7 the network 150. Thus, the central loghost 100 and the proxy loghost 160 are  
8 remote from each other. Appellant respectfully submits that this illustration and  
9 the disclosure of the instant Application, coupled with the definition from  
10 Wikipedia, further support the use of "remote" in the claims.

11 Further to the above, the instant Application has explicit disclosure that  
12 provides support for describing the central loghost and the proxy loghost as being  
13 remote from each other. For example, *paragraph [0024], line 5*, discloses "the  
14 remote proxy loghost."

15 The Office maintains the inclusion in **claim 12** of both "a plurality of  
16 proxy loghosts" and "a central loghost," where the "central loghost" receives "the  
17 log files themselves and the events from the plurality of proxy loghosts, the central  
18 loghost analyzing the log files and the events..." is not supported by the instant  
19 Application. The Appellant respectfully disagrees for the following reasons.

20 The proxy and central loghosts are independent modules (*See paragraph*  
21 *[0017], lines 1-2*), and stored log files and event files can be remotely accessed on  
22 proxy loghosts 160 and central loghosts 100 using https (*See paragraph [0018],*  
23 *lines 1-3*). Therefore, both loghosts 160 and 100 may include log files and event  
24 files.  
25

1 The proxy and central loghosts also include common software modules.  
2 (*See paragraph [0019], lines 1-2.*) For example, both loghosts 160 and 100  
3 include a "logsurf" module that is a real time log file analysis module that  
4 generates events and alerts. (*See paragraph [0021], lines 1-8; see also Fig. 2.*)  
5 Therefore, both loghosts 160 and 100 may generate events and alerts. In addition,  
6 both loghosts 160 and 100 may include a "syslog-ng" module (*See paragraph*  
7 *[0020], lines 1-7; see also Fig. 2.*) The syslog-ng module operating on proxy log  
8 hosts 160 is somewhat different from the syslog-ng module operating on central  
9 log host 100 in that the syslog-ng operating on proxy loghosts 160 is configured to  
10 receive log files and then forward event files to central loghost 100. (*See*  
11 *paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng on the central  
12 loghost 100 does not generally forward event files. Nonetheless, both syslog-ng  
13 modules may receive log files.

14 The above shows that both the proxy loghost 160 and the central loghost  
15 100 may be part of a common enterprise, and that the central log host 100 is  
16 capable of "analyzing the log files and the events," as is claimed, even when a  
17 proxy loghost 160 is implemented as part of the system. Therefore, at least the  
18 disputed subject matter of claim 12 is fully supported by the disclosure of the  
19 instant Application.

20 Appellant does not dispute that it "some cases" it "may" be beneficial to  
21 eliminate the use of proxy loghosts when an enterprise is sufficiently small. (*See*  
22 *paragraph [0031].*), as a small enterprise likely does not generate a sufficient  
23 volume of log files necessitating the use of the proxy loghosts. That is, the central  
24 loghost would likely provide sufficient log file handling for such an environment.  
25

1 However, this does not preclude the system claimed by claim 12, for example,  
2 when the enterprise is other than "sufficiently small."

3 For the reasons given above, the Board is asked to reconsider and withdraw  
4 of the 35 U.S.C. § 112, first paragraph, rejections.

5  
6 **(B) Claims 12-21 fully conform with the 35 U.S.C. § 112, first**  
7 **paragraph enablement requirement**

8  
9 **Independent claim 12**

10 The Office maintains the inclusion in **claim 12** of both "a plurality of proxy  
11 loghosts" and "a central loghost," where the "central loghost" receives "the log  
12 files themselves and the events from the plurality of proxy loghosts, the central  
13 loghost analyzing the log files and the events..." is not supported by the instant  
14 Application and thus the enablement requirement is not met. The Appellant  
15 respectfully disagrees for the following reasons.

16 The proxy and central loghosts are independent modules (*See paragraph*  
17 *[0017], lines 1-2*), and stored log files and event files can be remotely accessed on  
18 proxy loghosts 160 and central loghosts 100 using https (*See paragraph [0018],*  
19 *lines 1-3*). Therefore, both loghosts 160 and 100 may include log files and event  
20 files.

21 The proxy and central loghosts also include common software modules.  
22 (*See paragraph [0019], lines 1-2.*) For example, both loghosts 160 and 100  
23 include a "logsurf" module that is a real time log file analysis module that  
24 generates events and alerts. (*See paragraph [0021], lines 1-8; see also Fig. 2.*)  
25 Therefore, both loghosts 160 and 100 may generate events and alerts. In addition,

1 both loghosts 160 and 100 may include a "syslog-ng" module (*See paragraph*  
2 *[0020], lines 1-7; see also Fig. 2.*) The syslog-ng module operating on proxy log  
3 hosts 160 is somewhat different from the syslog-ng module operating on central  
4 log host 100 in that the syslog-ng operating on proxy loghosts 160 is configured  
5 to receive log files and then forward event files to central loghost 100. (*See*  
6 *paragraph [0020], lines 1-7; see also Fig. 2.*) The syslog-ng on the central  
7 loghost 100 does not generally forward event files. Nonetheless, both syslog-ng  
8 modules may receive log files.

9 The above shows that both the proxy loghost 160 and the central loghost  
10 100 may be part of a common enterprise, and that the central log host 100 is  
11 capable of "analyzing the log files and the events," as is claimed, even when a  
12 proxy loghost 160 is implemented as part of the system. Therefore, at least the  
13 disputed subject matter of claim 12 is fully enabled by the disclosure of the instant  
14 Application.

15 Appellant does not dispute that it "some cases" it "may" be beneficial to  
16 eliminate the use of proxy loghosts when an enterprise is sufficiently small. (*See*  
17 *paragraph [0031].*), as a small enterprise likely does not generate a sufficient  
18 volume of log files necessitating the use of the proxy loghosts. That is, the central  
19 loghost would likely provide sufficient log file handling for such an environment.  
20 However, this does not preclude the system claimed by claim 12, for example,  
21 when the enterprise is other than "sufficiently small."

22 For the reasons given above, the Board is asked to reconsider and withdraw  
23 of the 35 U.S.C. § 112, first paragraph, rejection.  
24  
25

1 (C) Claims 1-12 recite statutory subject matter, as required under  
2 35 U.S.C. § 101  
3

4 Independent claims 1 and 12

5 The Office maintains the recitation in claims 1 and 12 "would be  
6 reasonably interpreted by one of ordinary skill in the art as software, per se."  
7 Appellant respectfully disagrees for the following reasons.

8 Claim 1 recites "a plurality of resources operating on the network" and  
9 claim 12 recites a central loghost in communication with a plurality of loghosts  
10 "over a network" Appellant respectfully submits, in consideration of the foregoing  
11 language alone, that one of ordinary skill in the art would not conclude that the  
12 rejected claims are directed solely to software. In particular, those of ordinary  
13 skill in the computer art readily understand networks generally comprise various  
14 hardware components (e.g., computers and routers), not software alone as  
15 suggested by the Office. The Appellant's own disclosure makes this point. (*See*  
16 *e.g., paragraph [0015].*)

17 Moreover, Appellant previously amended the claims 1 and 12 to include the  
18 recitation "computer-implemented system." The Office has refused to give any  
19 weight to the added subject matter when determining whether the claims recite  
20 statutory subject matter. However, such an approach is inconsistent with  
21 established law. In particular, a "computer-implemented system" is clearly a  
22 physical thing, and 35 U.S.C. § 101 statutory subject matter includes "new and  
23 useful" machines.

24 Further, the Office has recognized that such subject matter (e.g., methods  
25 embodied on computer-readable media) in the preamble renders process or method

1 claims as being at the very least statutory subject matter under 35 U.S.C. § 101.  
2 Therefore, the rejected claims require the same recognition.

3 For the reasons given above, the Board is asked to reconsider and withdraw  
4 of the 35 U.S.C. § 101 rejection.

5  
6 **(D) Claims 1-7, 9-17, 19-28 and 30 are allowable because Khanolkar**  
7 **does not suggest the subject matter of these claims**

8  
9 **Independent claims 1, 12 and 22 & dependent claim 9**

10 Each of the rejected independent claims 1, 12 and 22 recites that the  
11 central and proxy loghosts are "remote" from each other. As discussed earlier  
12 herein, and as is shown in Fig. 1 of the instant Application, the central loghost 100  
13 and the proxy loghost 160 are separated by the network 150. Thus, the central  
14 loghost 100 and the proxy loghost 160 are remote from each other. Khanolkar  
15 does not suggest this remote configuration.

16 Khanolkar describes event parsers 54 and an event manager 55 that are part  
17 of the *same* system 10 and also part of the *same* subsystem 50. (*See Khanolkar,*  
18 *col. 3, lines 49-58; Fig. 2.*) Certainly, the event parsers 54 and the event manager  
19 55 are not separated by a network. Therefore, the parsers 54 and the event  
20 manager 55 are not remote from each other.

21 Further to the above, claim 12 recites that the central loghost receives and  
22 analyzes log files and events. Khanolkar fails to suggest a central loghost that  
23 receives log files and events, and instead only discloses the event manager 55 as  
24 receiving event objects, not log files as claimed.

1        Regarding **claim 9**, the recitation of this claim provides for the separate  
2 archival of log files and events. In particular, the archiving of log files on the  
3 proxy loghost and the archiving of events on the central loghost, and where the  
4 two loghosts are remote from each other (see claim 1). Such a storage  
5 arrangement is not suggested by Khanolkar. In particular, Khanolkar suggests  
6 event parsers 54 and the event manager 55 as part of the same event handling  
7 subsystem 50 and suggests a database 58 as storing only event objects (not log  
8 data). (See *Khanolkar col. 7, lines 10-12 & lines 23-36.*)

9        Those claims not discussed in particular in the foregoing, are at least  
10 allowable due to their dependence upon one of the independent claims discussed  
11 hereinabove.

12        For the reasons given above, Khanolkar does not suggest the subject matter  
13 of the rejected claims. Hence, for at least this reason, these claims are allowable.

14  
15        **(E) Claims 8, 18 and 29 are allowable because Khanolkar in view**  
16        **APA does not suggest the subject matter of these claims**

17        At the very least, claims 8, 18 and 29 are allowable due to their dependence  
18 upon an allowable independent claim. Moreover, the APA does not remedy the  
19 deficiencies discussed herein in connection with Khanolkar. Hence, for at least  
20 this reason, these claims are allowable.

1       **Conclusion**

2       Claims 1-30 are in condition for allowance. Appellant respectfully requests  
3       reconsideration and withdrawal of the rejections and prompt allowance of the  
4       subject application.  
5

6  
7                               Respectfully Submitted,

8                               Lee & Hayes, PLLC  
9

10       Date: March 12, 2008

11       By: Tim R. Wyckoff/  
12               Tim R. Wyckoff  
13               Attorney at Law  
14               Reg. No. 46,175  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25



**(viii) Claims Appendix**

1  
2  
3 1. **(Previously Amended)** A computer-implemented monitoring/intrusion  
4 detection system, comprising:

5 a central loghost,

6 at least one proxy loghost remote from the central loghost and in  
7 communication with the central loghost over a network; and

8 at least one monitoring station,

9 wherein the proxy loghost receives a plurality of log files from a plurality  
10 of resources operating on the network, analyzes the log files for at least one of  
11 unexpected volume, unexpected patterns, or unexpected types of log files, and  
12 generates events in view of such analysis,

13 wherein the central loghost is operable to receive the events generated by  
14 the proxy loghost through the network and generate an alert upon an analysis of  
15 the events, and

16 wherein the monitoring station is caused to issue an alarm when the alert is  
17 generated.

18  
19 2. **(Original)** The system of claim 1, wherein the central loghost comprises  
20 a plurality modules operating in a Unix environment.

21  
22 3. **(Original)** The system of claim 1, further comprising a plurality of proxy  
23 loghosts, each one of the plurality being in communication with the central  
24 loghost.  
25

1           4. **(Original)** The system of claim 1, wherein the resources comprise at  
2 least one of an operating system, application, firewall, router, switch and  
3 loadbalancer.

4  
5           5. **(Original)** The system of claim 1, wherein a plurality of events is  
6 required to cause the generation of an alert.

7  
8           6. **(Original)** The system of claim 1, wherein security management has  
9 access to both the proxy loghost and the central loghost.

10  
11          7. **(Original)** The system of claim 1, wherein the log files are received from  
12 a network-based intrusion detection system.

13  
14          8. **(Original)** The system of claim 1, wherein the log files are received from  
15 a host-based intrusion detection system.

16  
17          9. **(Original)** The system of claim 1, wherein the log files are archived on  
18 the proxy loghost and the events are archived on the central loghost.

19  
20          10. **(Original)** The system of claim 1, further comprising software adapters  
21 to convert one format of a log file to another format.

22  
23          11. **(Original)** The system of claim 1, further comprising a module for  
24 visualizing the log files received at the proxy loghost.

1           12. **(Previously Amended)** A computer-implemented system for detecting  
2 intrusion into a secure network, comprising:

3           a plurality of proxy loghosts, each proxy loghost collecting log files that are  
4 generated by resources in a portion of the secure network, the plurality of loghosts  
5 generating events in response to the log files collected; and

6           a central loghost remote from the plurality of proxy loghosts and in  
7 communication with the plurality of proxy loghosts over a network, the central  
8 loghost receiving the log files themselves and the events from the plurality of  
9 proxy loghosts, the central loghost analyzing the log files and the events to  
10 determine the necessity of generating an alert and an associated alarm to notify a  
11 security manager of a possible intrusion incident.

12  
13           13. **(Original)** The system of claim 12, wherein the central loghost  
14 comprises a plurality modules operating in a Unix environment.

15  
16           14. **(Original)** The system of claim 12, wherein the resources comprise at  
17 least one of an operating system, application, firewall, router, switch and  
18 loadbalancer.

19  
20           15. **(Original)** The system of claim 12, wherein a plurality of events is  
21 required to cause the generation of an alert.

22  
23           16. **(Original)** The system of claim 12, wherein security management has  
24 access to both the plurality of proxy loghosts and the central loghost.  
25

1           17. **(Original)** The system of claim 12, wherein the log files are received  
2 from a network-based intrusion detection system.

3  
4           18. **(Original)** The system of claim 12, wherein the log files are received  
5 from a host-based intrusion detection system.

6  
7           19. **(Original)** The system of claim 1, wherein the log files are archived on  
8 the plurality of proxy loghosts and events are archived on the central loghost.

9  
10          20. **(Original)** The system of claim 12, further comprising software  
11 adapters to convert one format of a log file to another format.

12  
13          21. **(Original)** The system of claim 12, further comprising a module for  
14 visualizing the log files received at the proxy loghost.

15  
16          22. **(Previously Amended)** A method of monitoring a network,  
17 comprising:

18           receiving a plurality of log messages at a proxy loghost;  
19           analyzing the log messages and determining whether, in the log files, there  
20 exists any anomalies or unusual patterns;

21           generating an event in response to the anomalies or unusual patterns and  
22 forwarding the event over a network from the proxy loghost to a remote central  
23 loghost;

24           monitoring the events at the central loghost and generating an alert in  
25 accordance with predetermined event analysis; and

generating an alarm communication in coordination with the alert, the alarm being indicative of an unwanted incident in the network.

23. **(Original)** The method of claim 22, wherein the central loghost comprises a plurality modules operating in a Unix environment.

24. **(Original)** The method of claim 22, wherein a plurality of proxy loghosts receive log files.

25. **(Original)** The method of claim 22, wherein the log files are received from resources comprising at least one of an operating system, application, firewall, router, switch and loadbalancer.

26. **(Original)** The method of claim 22, further comprising generating the alert only after a plurality events are received.

27. **(Original)** The method of claim 22, further comprising remotely accessing, from a single location, both the proxy loghost and the central loghost.

28. **(Original)** The method of claim 22, wherein the log files are received from a network-based intrusion detection system.

29. **(Original)** The method of claim 22, wherein the log files are received from a host-based intrusion detection system.

1           30. **(Original)** The method of claim 22, further comprising archiving the  
2 log files on the proxy loghost and archiving the event on the central loghost.  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

**(ix) Evidence Appendix**

None.

**(x) Related Proceedings Appendix**

None.